LISTEN.
THINK.
SOLVE.®

PlantPAx
Process Automation System

PR04 – PlantPAx

过程安全介绍

Process Solutions Team (China)

Allen-Bradley • Rockwell Software

Rockwell Automation

Agenda

- 安全定义
- 什么是SIL
- ICS Triplex
- 安全应用

什么是功能性安全?

系统功能安全主要是以保护人身财产安全为目的
与安全相关的保护系统，其包括安全控制系统和安全保护系统

设备

1. 连续的运动
2. 停止

连续的过程

1. 停止
2. 维护控制

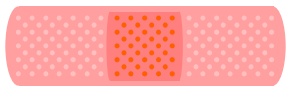
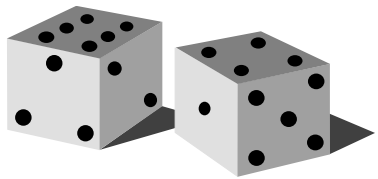
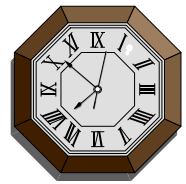
Agenda

- 安全定义
- 什么是SIL
- ICS Triplex
- 安全应用

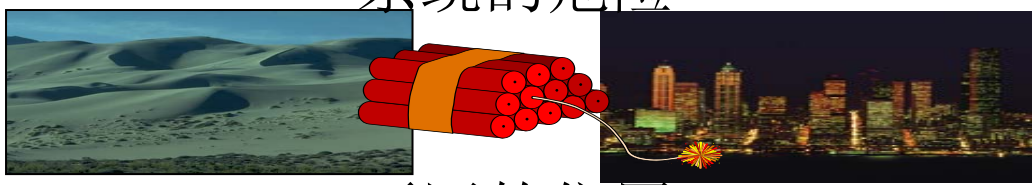
SIL(Safety Integrity Level)
是量化风险的一种方法

危险/安全
安全
环境
经济/PR

风险降低

多么严重?	多么可能?	多经常?
		
结果	机会	频率

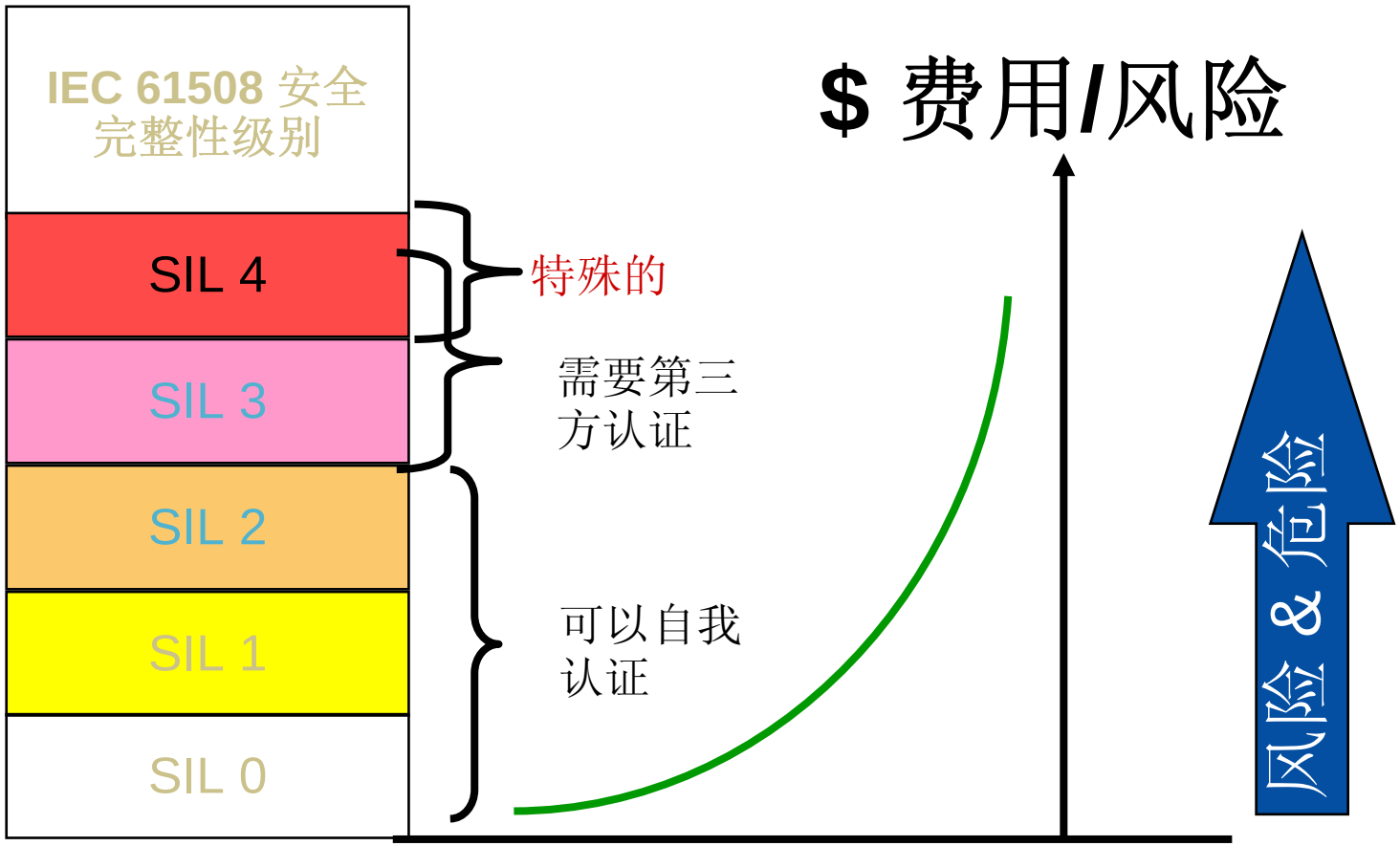
系统的危险



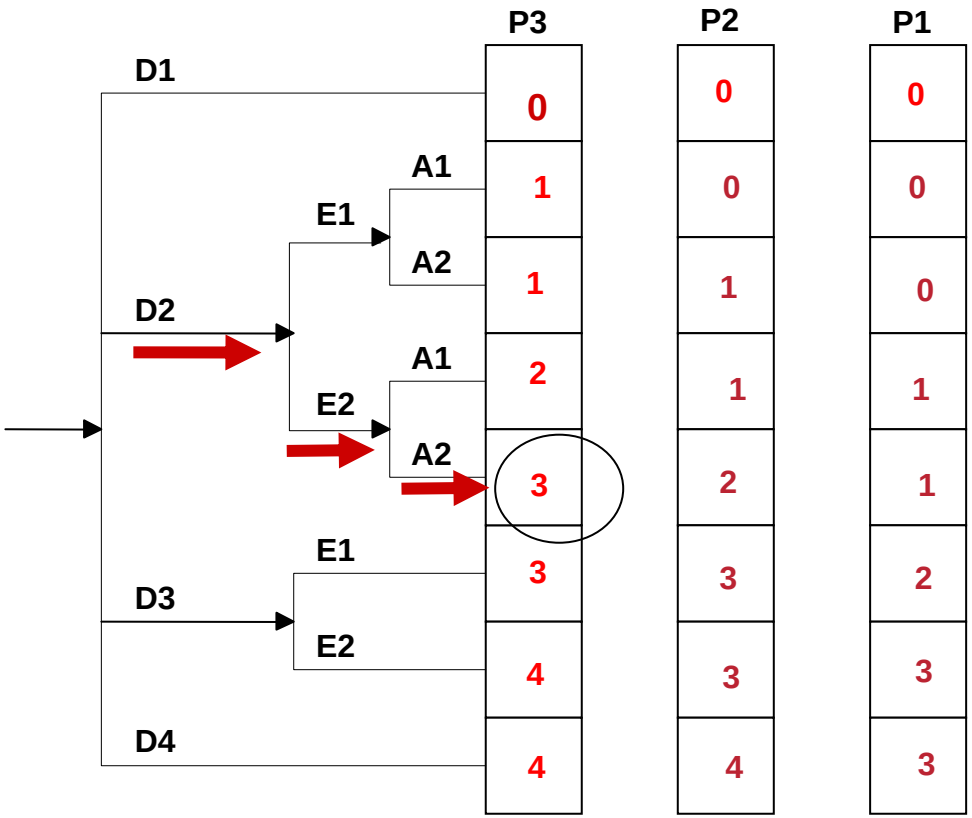
不同的位置

SIL安全完整性级别

量化风险的方式



风险评估-决定/SIL



风险参数:

D - 破坏程度

D1: 轻微伤害
D2: 造成一人或多人的严重伤害或造成一人死亡
D3: 多人死亡
D4: 灾难性后果，多人死亡

E - 暴露时间

E1: 很少到相对频繁
E2: 频繁到持续不断

A - 危险避免/缓解

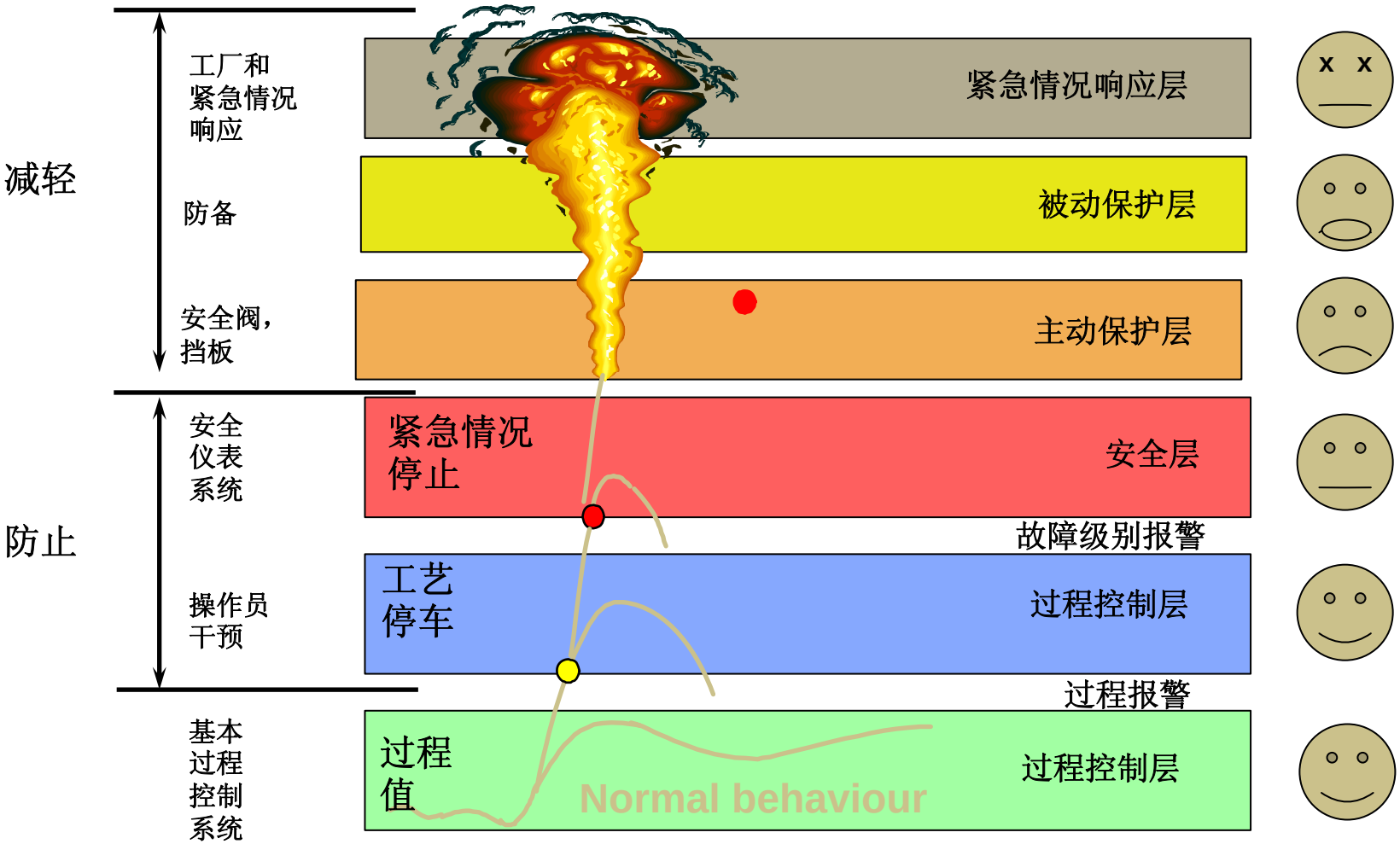
A1: 可能在一定的条件下
A2: 很小可能

P - 出现可能性

P1: 非常低的可能性
P2: 低可能
P3: 相对高可能

Source: TUV Product Service

分层防护的安全机制



典型的安全应用

- ESD: 紧急停车系统
- PSD: 生产停车系统
- BMS: 燃烧管理系统
- F&G: 火灾& 天然气检测& 灭除系统
- HIPPS: 高压保护
- CPC: 关键过程控制
- TMC: 透平和压缩机控制

过程安全

- 几乎所有工业
  - 锅炉燃烧管理系统(BMS)
- 许多重工业
  - 透平 / 压缩机
- 石油 & 天然气
  - ESD, F&G, TMC, HIPPS
- 能源
  - 涡轮过电压保护
  - BMS
- 采矿
  - 在采矿处理中的ESD

应用的过程控制安全标准

- IEC 61508 电器/电子/可编程电子安全相关系统的功能性安全
- IEC 61511 功能性安全: 过程工业部分的安全仪表系统
- ANSI/ISA S.84.01 与 IEC 61511 相同，包含了以前版本的条款

- NFPA 72国家火灾保护协会第72部分火灾保护系统
- NFPA 85.01 国家火灾保护协会85.01，用于单个燃烧锅炉的熔炉爆炸/爆裂的标准。
- NFPA 85.02标准，用于防止多个单体燃烧锅炉熔炉爆炸/爆裂。
- NFPA 86标准，用于燃烧炉控制

- EN 50178 用于电力能源安装的电气设备
- EN 50156 用于燃烧炉的电气设备
- EN 54-2 火灾检测和报警系统

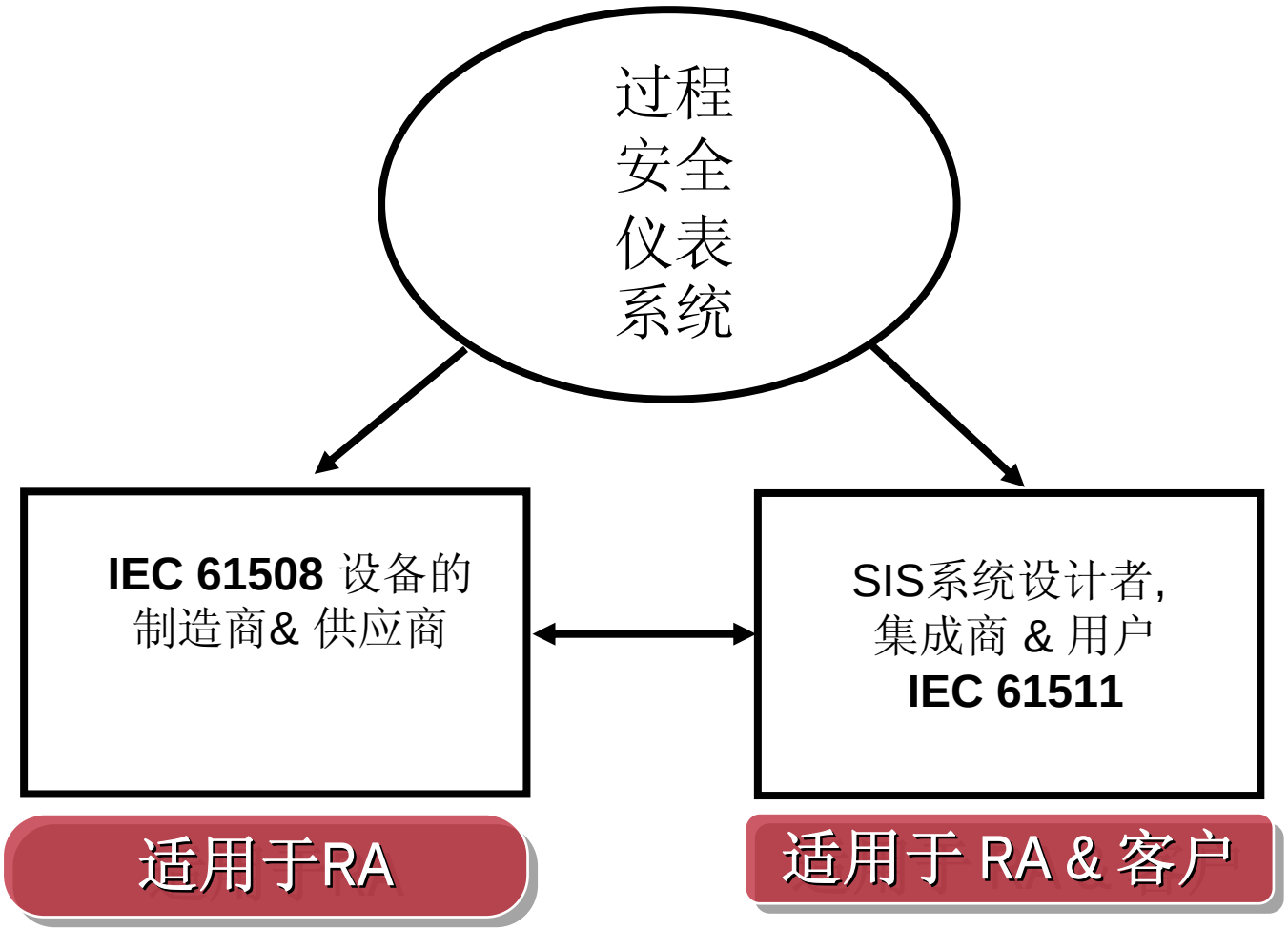
- DIN VDE 0801用于安全相关系统的计算机准则
- DIN VDE 19250 对于设备进行测量和控制时需要考虑的基本方面
- DIN VDE 0116 燃烧炉电气设备

- API 美国石油协会

应用的过程控制安全标准

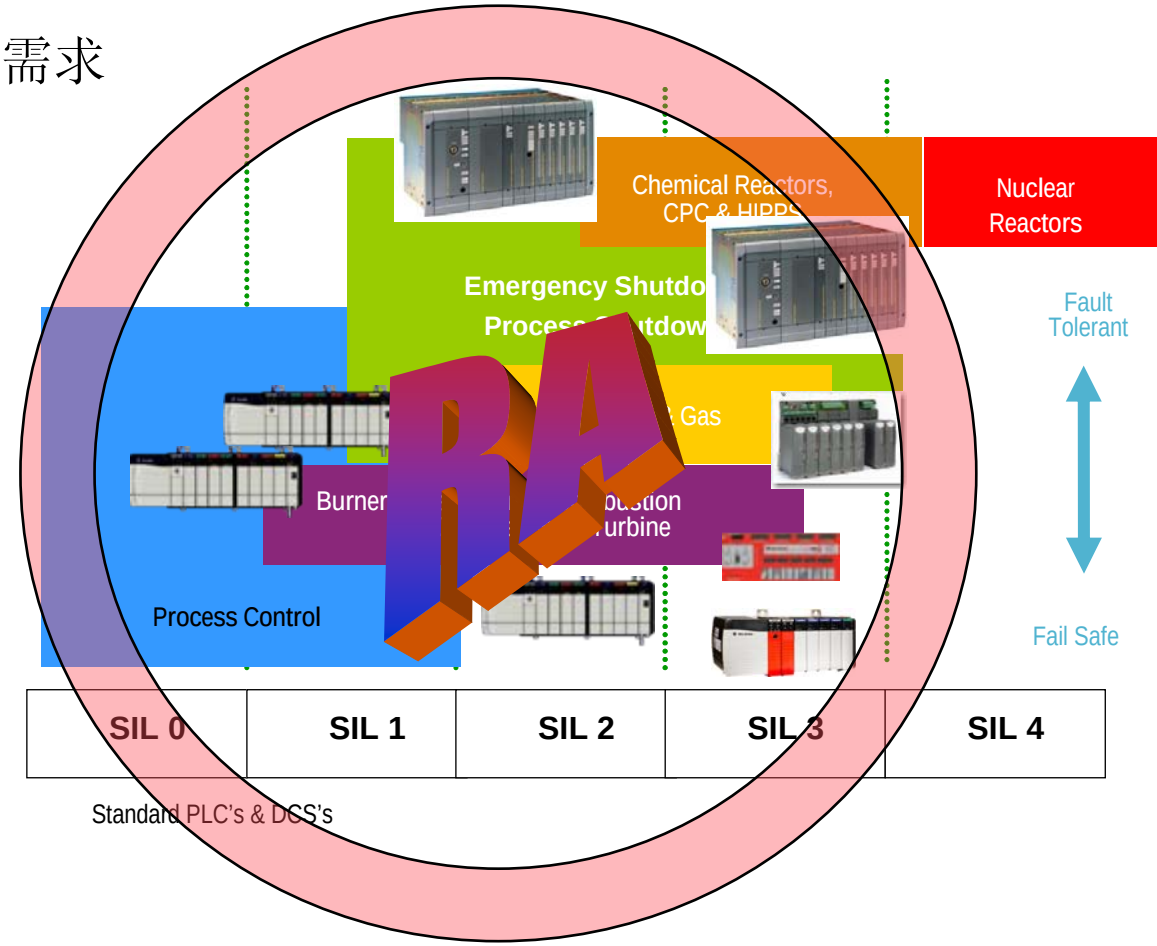
- IEC 61508电器/电子/可编程电子安全相关系统的功能性安全
- 本标准是基于安全相关系统的可靠性，它是安全相关系统功能安全的基础标准，有七个部分组成，描述了安全相关系统的软硬件的要求（从危险分析和安全功能的详细说明开始，直到系统停用和处理）。它提出了4个安全完整性等级。提出了影响安全完整性等级的二个因素，安全故障的比例和目标失效量的测量。
- IEC 61511 功能性安全: 过程工业部分的安全仪表系统
- 本标准是IEC61508 在过程工业领域的应用。本标准给出了安全仪表系统的规范、设计、安装、运行和维护要求；以及它的应用指南和确定要求的安全完整性等级的指南。主要适用于包括化工、炼油、油气生产、纸浆和造纸等在内的过程控制领域：它适用于安全仪表系统的设计师、集成商和用户。

国际过程安全标准



PlantPAx: 过程安全控制产品

- 各种规模的解决方案满足不同需求
- 通用或专用的产品
- 分立或成套
  - OPC 及 FactoryTalk
  - CIP
- 满足SIL1, 2 和 3的解决方案.
  - 实效—安全型
  - 容错型
- 不同冗余配置满足不同要求:
  - 1oo1
  - 1oo2, 2oo2
  - 2oo3

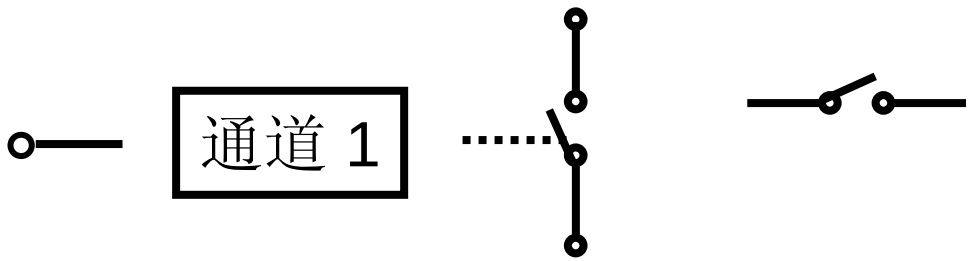


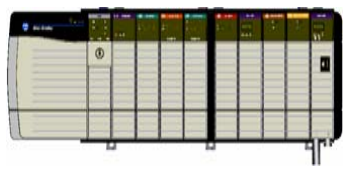
基本架构

通道 =

单重化 1oo1

容错=0

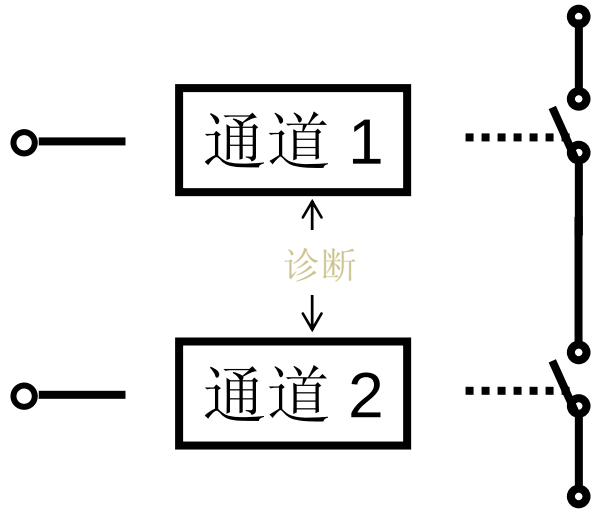




基本架构

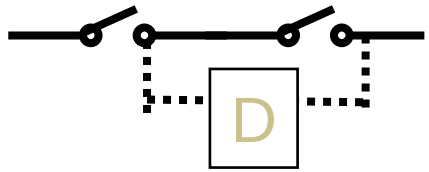
双重化 1oo2

双重化1oo2d

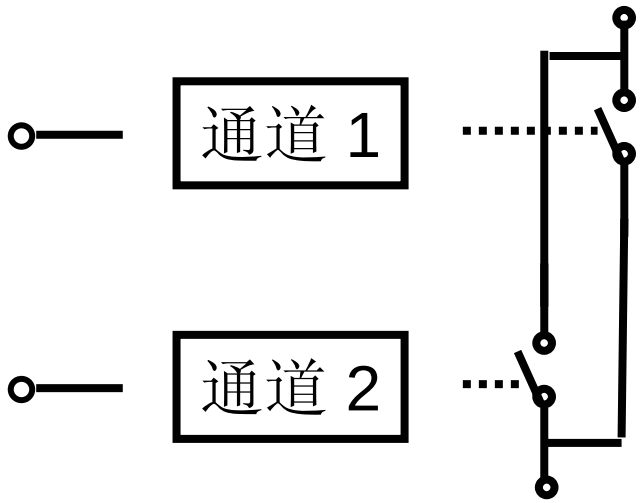


容错 = 1

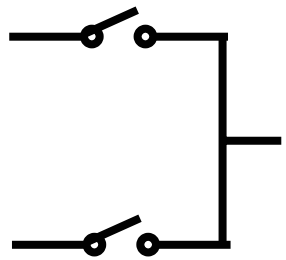
两个带有冗余
输出的通道
串联来
确保安全关断



双重化2oo2

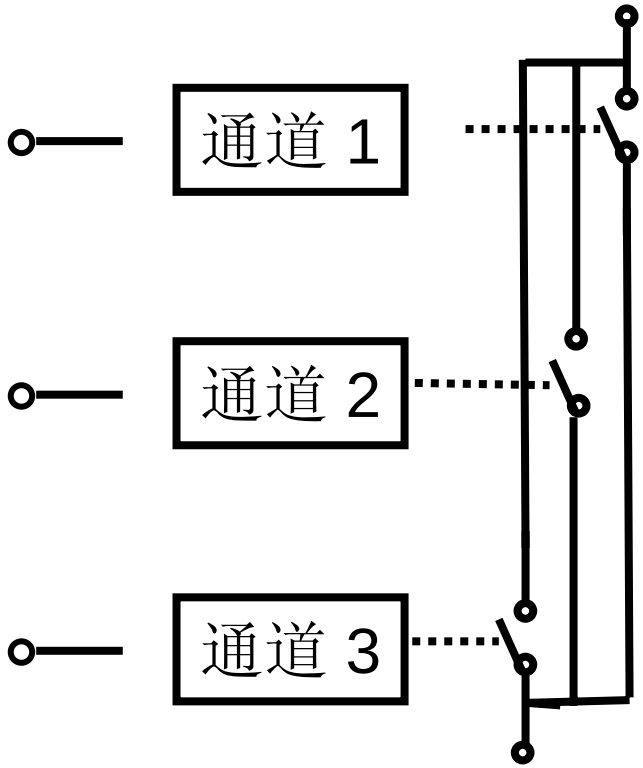


两个带有冗余
输出的通道
并联来
确保可用性

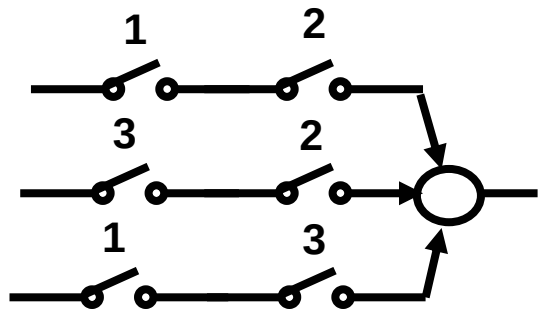


基本架构

三重化 2oo3



三个带有冗余输出
的通道并联和投票

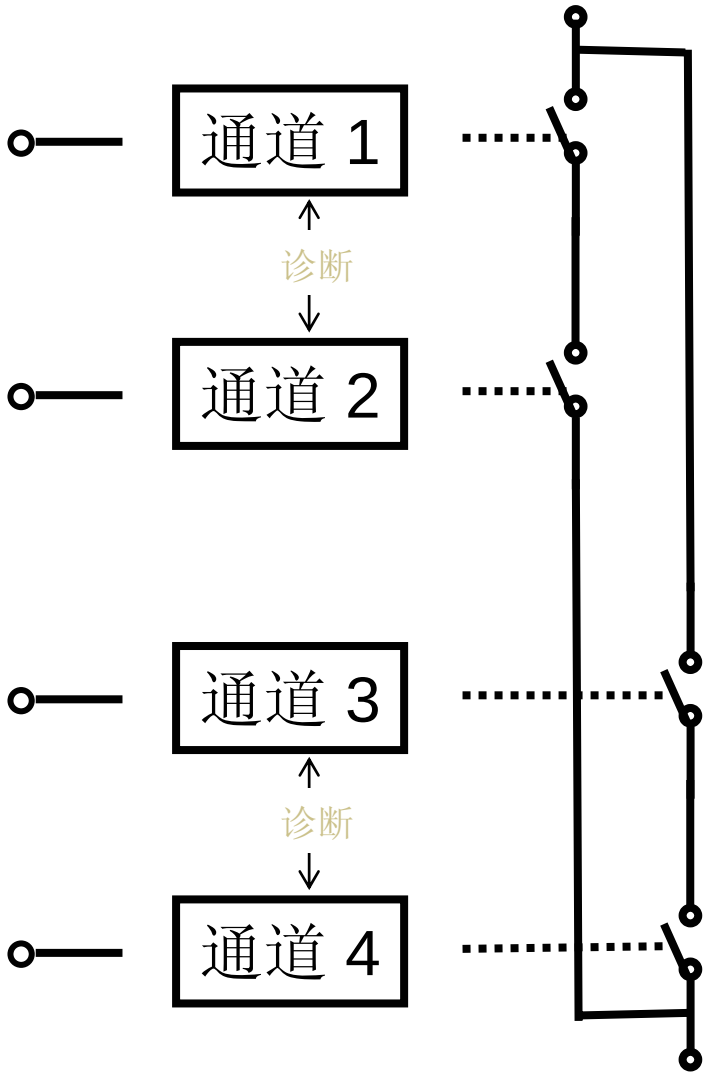


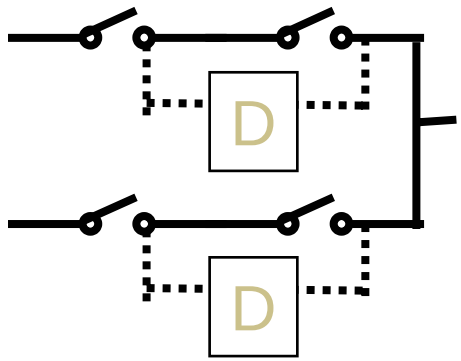
TMR 总线三重化冗余

基本架构

四重化?

双重化!

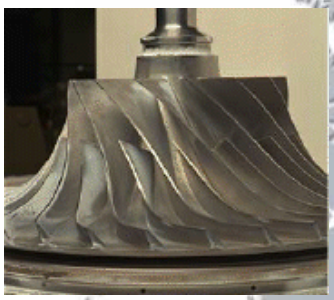


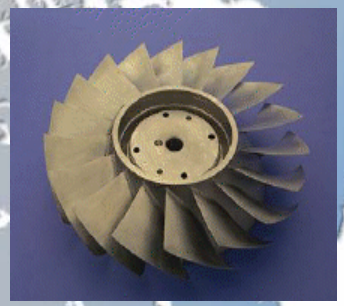


Agenda

- 安全定义
- 什么是SIL
- ICS Triplex
- 安全应用

2007年6月RA收购ICS Triplex





Aberdeen, **UK**

Maldon, Horsham & Coventry, **UK**

Paris, **France**

Grenoble, **France**

Montreal, **Canada**

Milan, **Italy**

Beijing, **China**

Houston, **USA**

Al Khobar, **KSA**

Dubai, **UAE**

Mexico City, **Mexico**

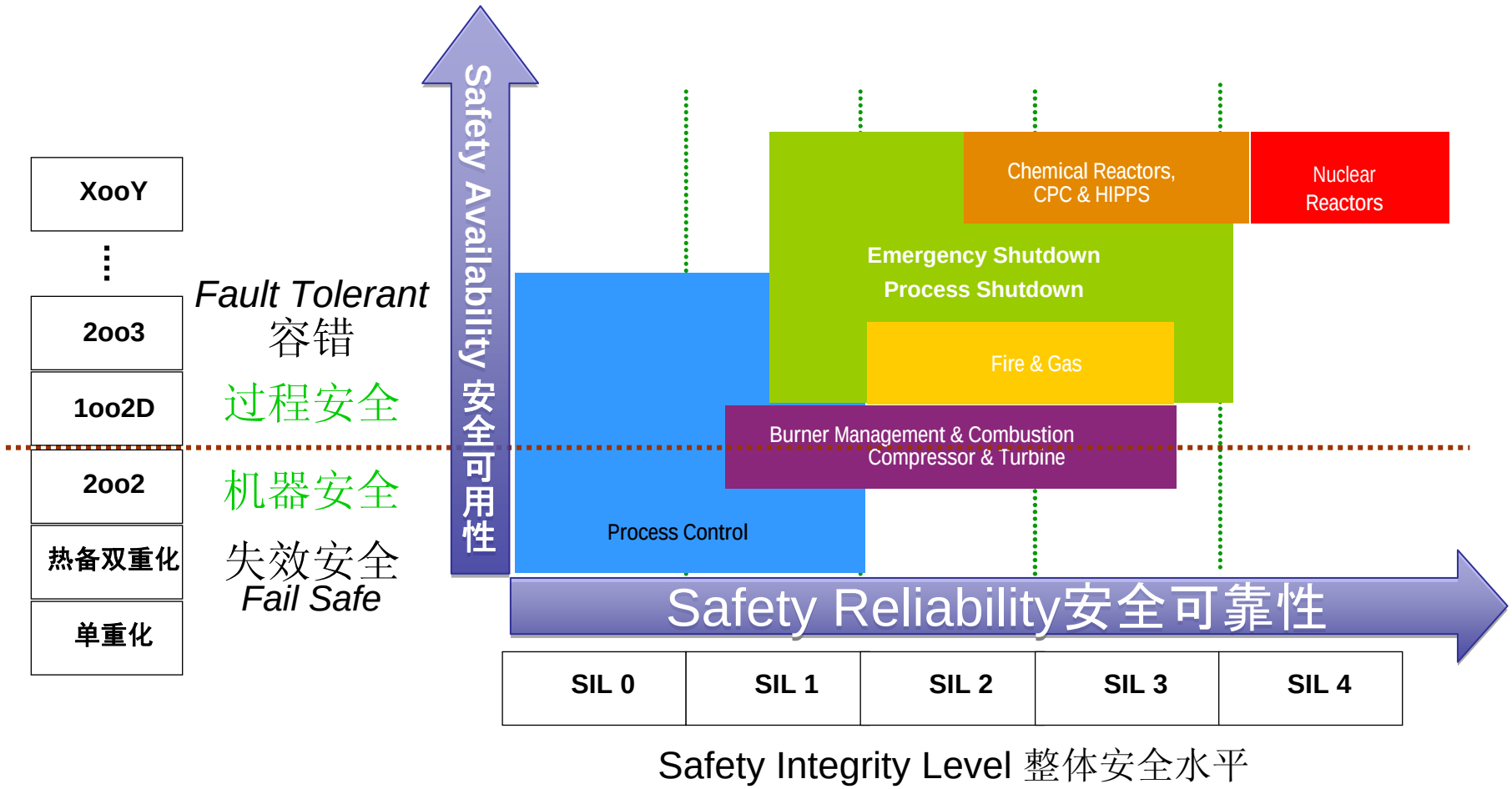
Abu Dhabi, **UAE**

Kuala Lumpur, **Malaysia**

Singapore

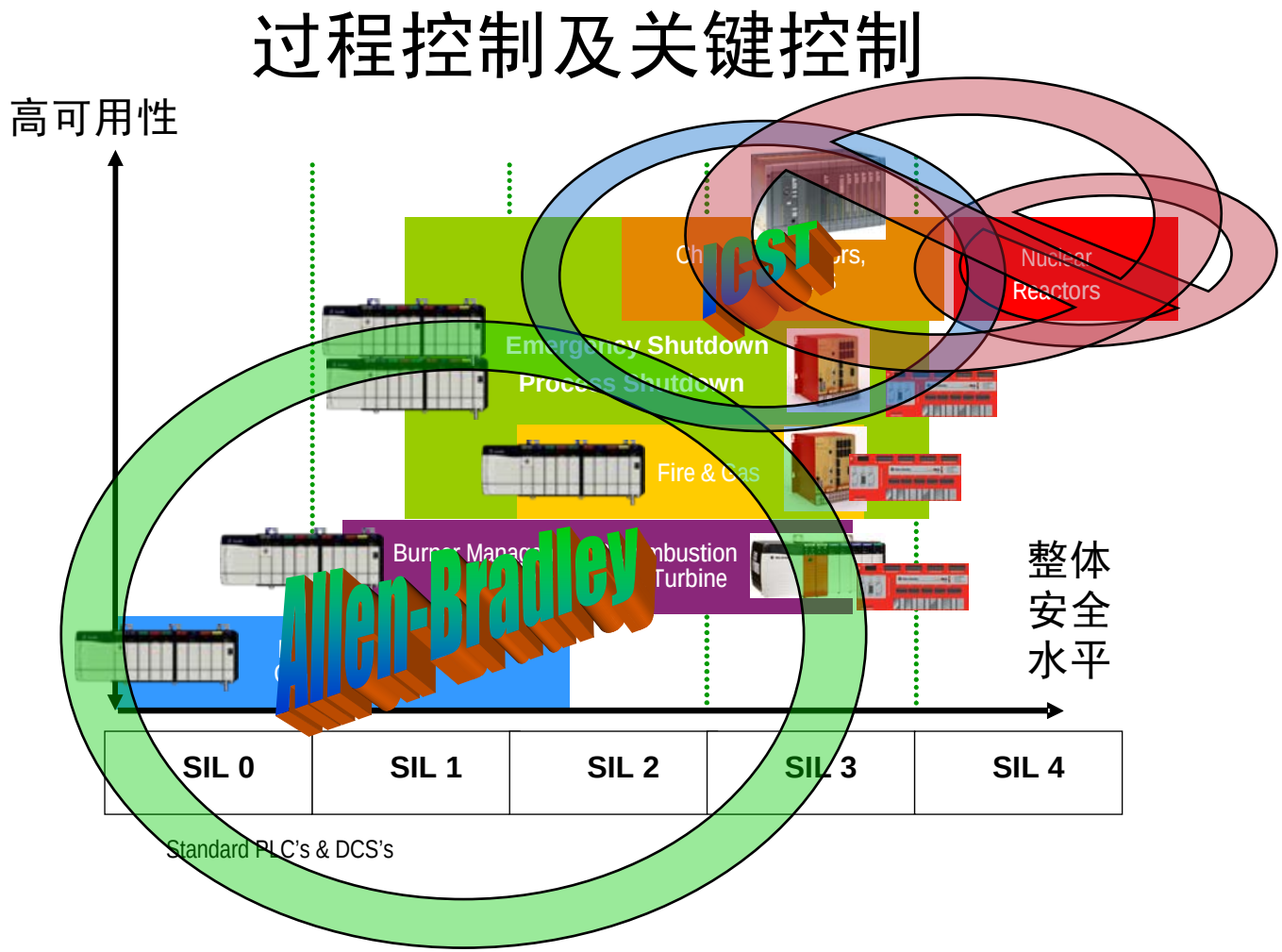
Perth, **Australia**

过程控制及关键控制分野

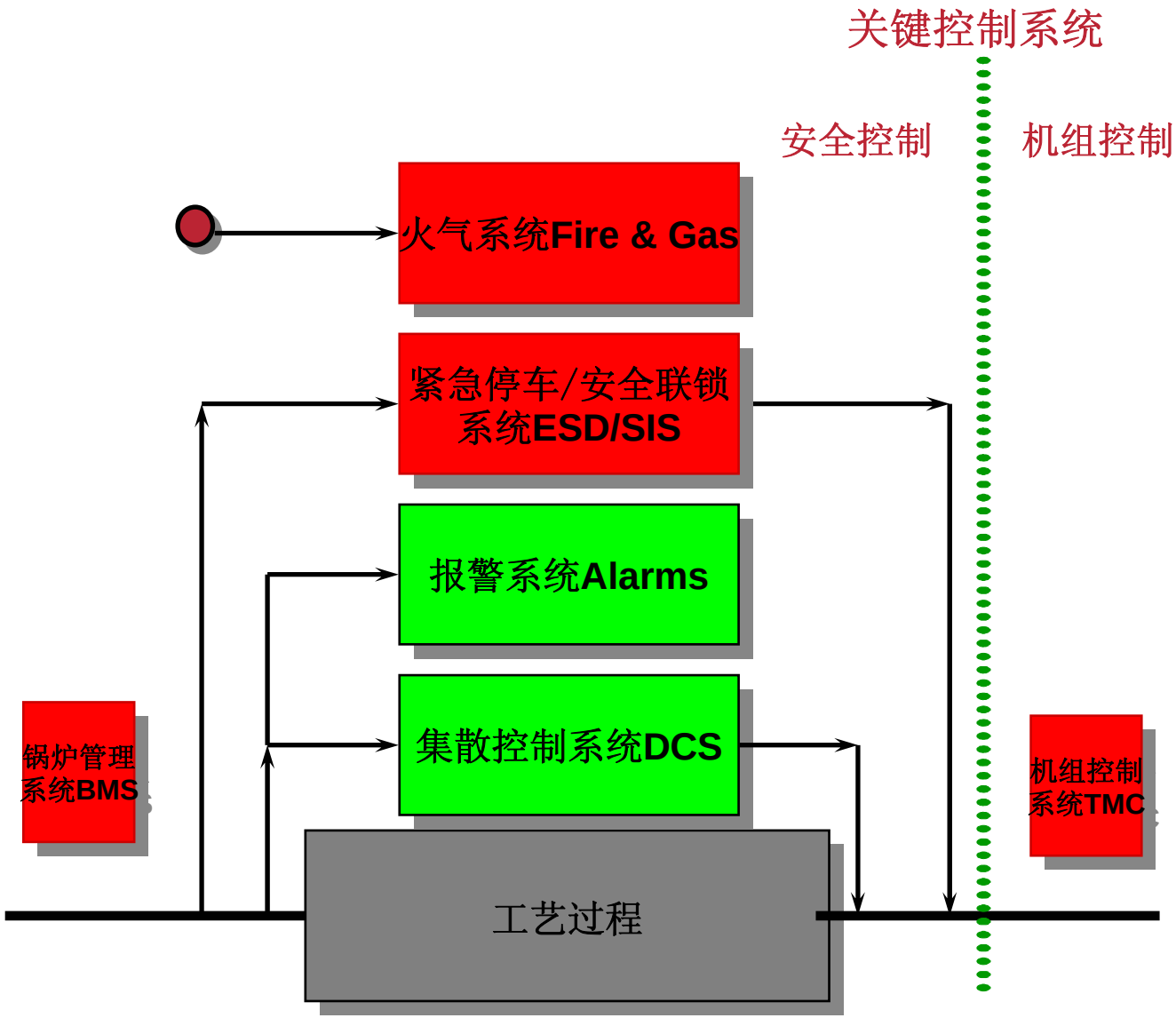


罗克韦尔解决方案所覆盖的领域

- 现在...



关键控制系统



罗克韦尔ICS Triplex的贡献

（生命攸关的）关键控制系统 (Life) Critical Control

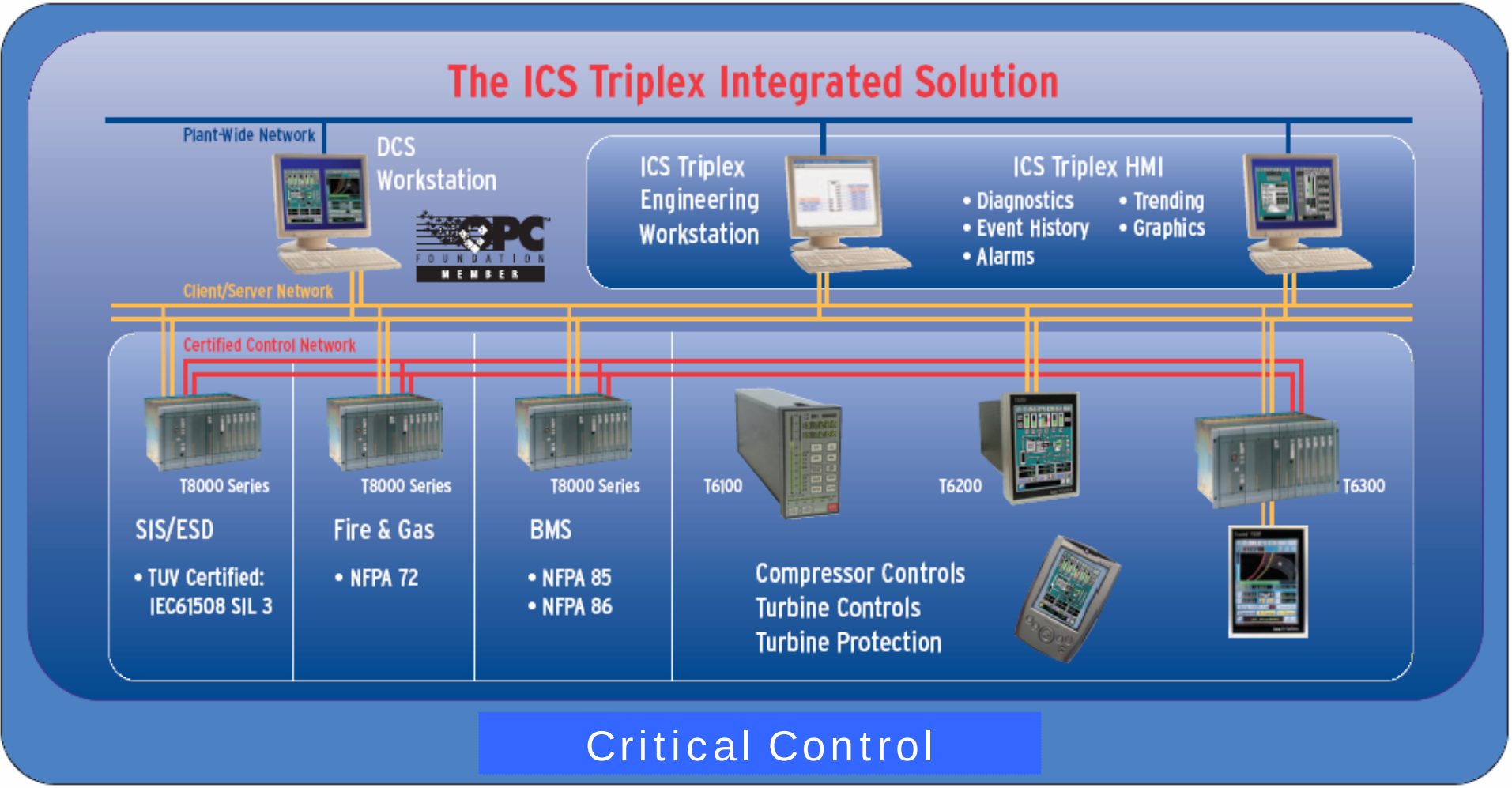
紧急停车/安全联锁系统ESD/SIS

火气监测/保护系统 Fire&Gas Detection/Protection

锅炉管理系统BMS

机组控制系统TMC

ICS Triplex关键控制整体解决方案



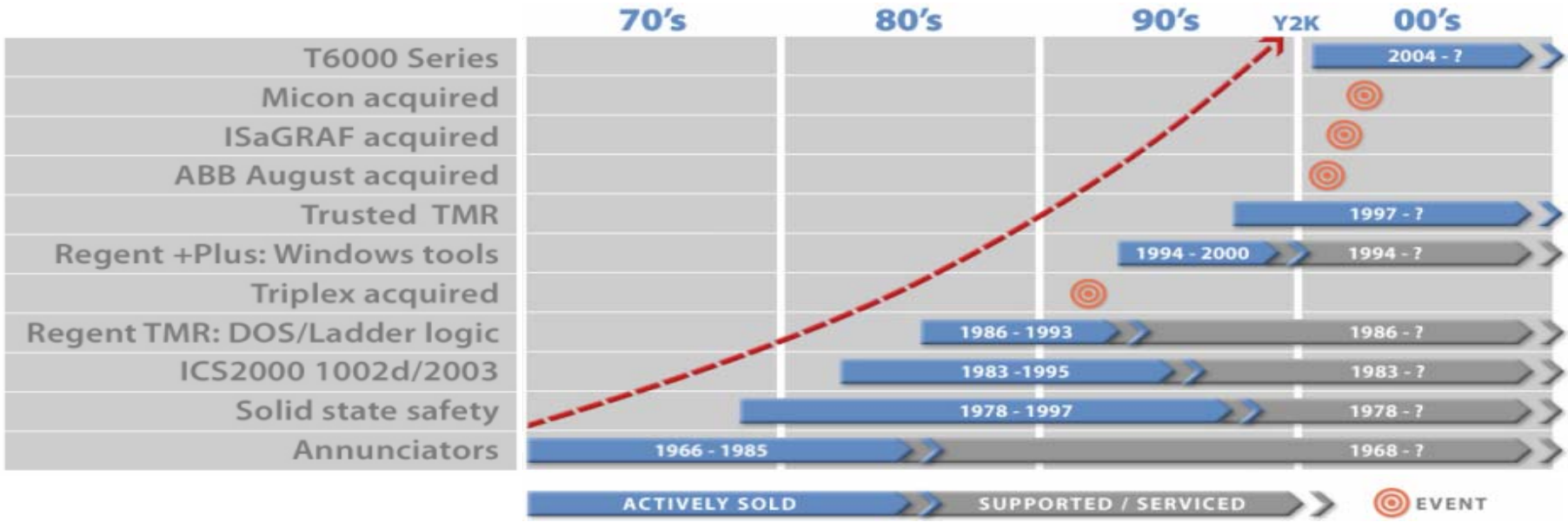
硬件平台 – 技术演化

1977 – T6200

1986 – Regent
1994 - Regent+plus

1998 - Trusted

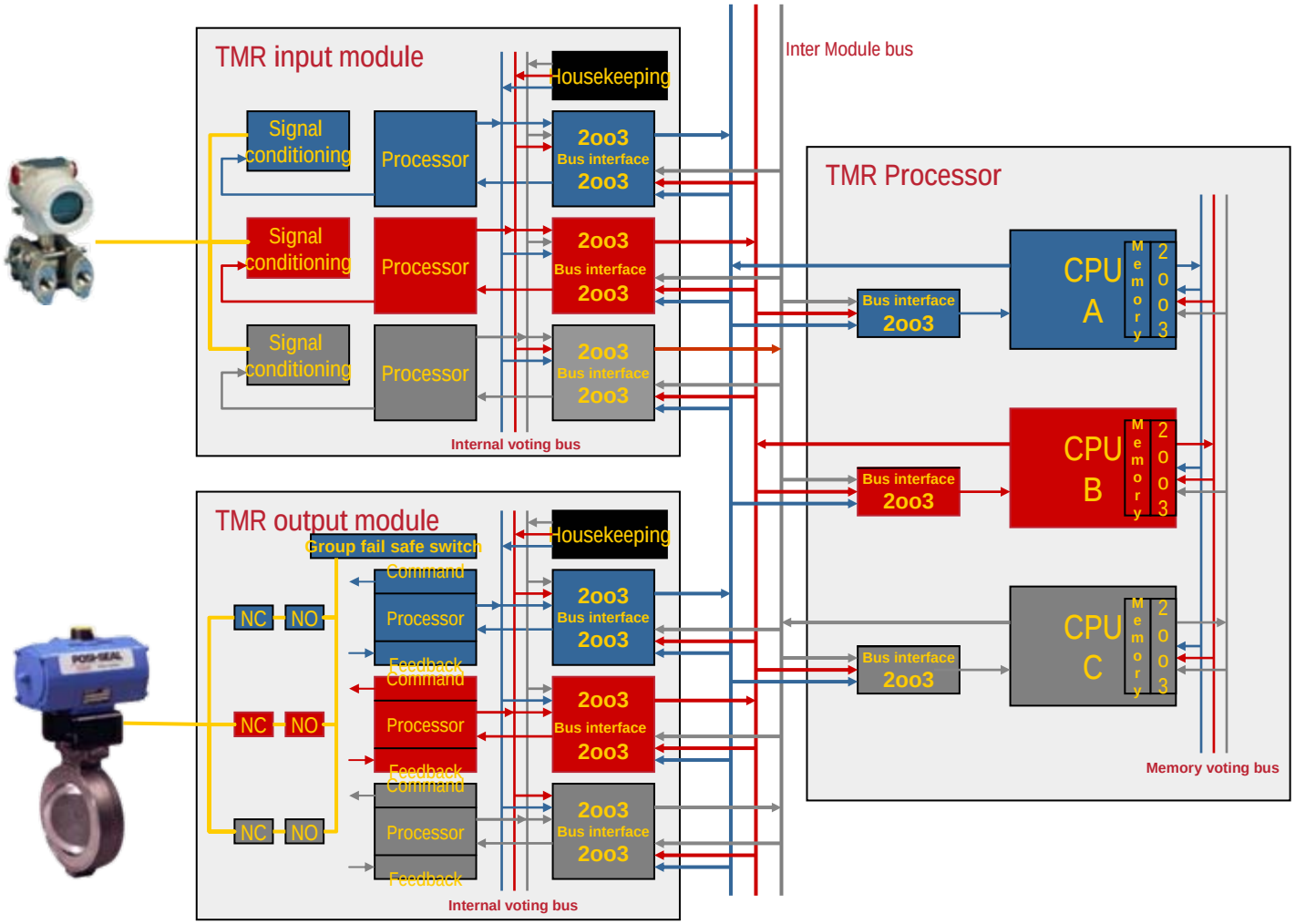
2008 - AADvance



Trusted关键控制系统

- 多个应用领域：ESD/SIS/F&G/TMC
- TMR (Triple Mainbus Redundant)总线三重化容错高度自诊断、高可靠性、高可用性
- 独有的 3-3-2-2-0降级模式
- TUV SIL 3认证
- 控制器之间的对等通讯获得认证
- IRIG-B 方式实现大范围多系统时钟同步
- 所有模块均可以在线热更换
- 通用I/O模块：DI/DO/AI/AO
- 专用I/O模块：火气、阀门测试、机组控制
- I/O模块来实现1毫秒的事件序列(SOE)分辨率
- IEC 61131-3编程环境
- 应用程序在线上传、修改、下装

Trusted HIFT硬件结构拓扑图



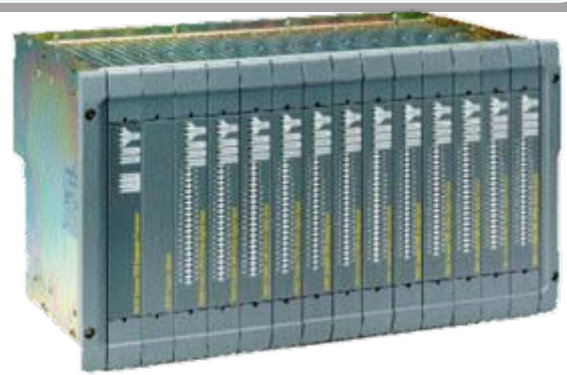
Trusted控制机架及扩展机架

控制机架

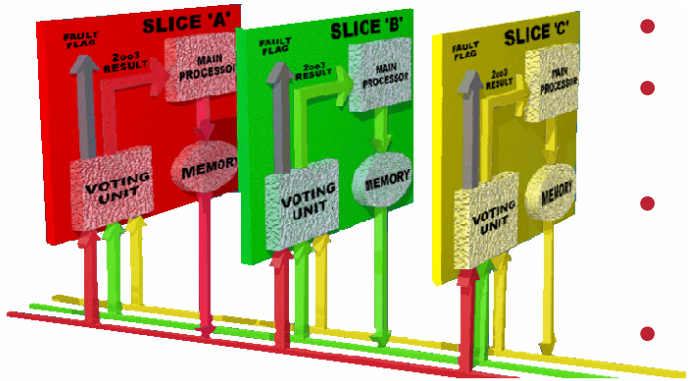
扩展机架

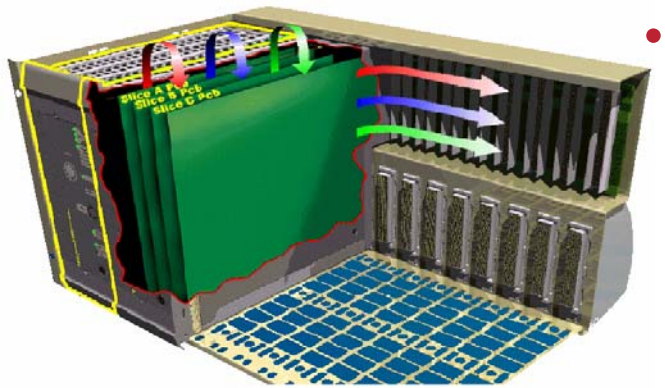
Companion Slot 相邻槽方式排布

Smart Slot 智能槽方式排布



Trusted硬件 – 处理器模块





- 一块模块内部三重化
- 3-2-0或3-3-2-2-0 降级模式
- 64位Motorola RISC 微处理器(600系列)
- 快速处理及扫描能力
- 无扰动热更换
- 可热更换
- 可带双Modbus端口
  - 1 RS422/485 2线
  - 2 RS422/485 2 or 4线
- IRIG-B 时钟同步

Trusted硬件 – 常用I/O模块 （DI/DO/AI/AO）

输入/输出模块

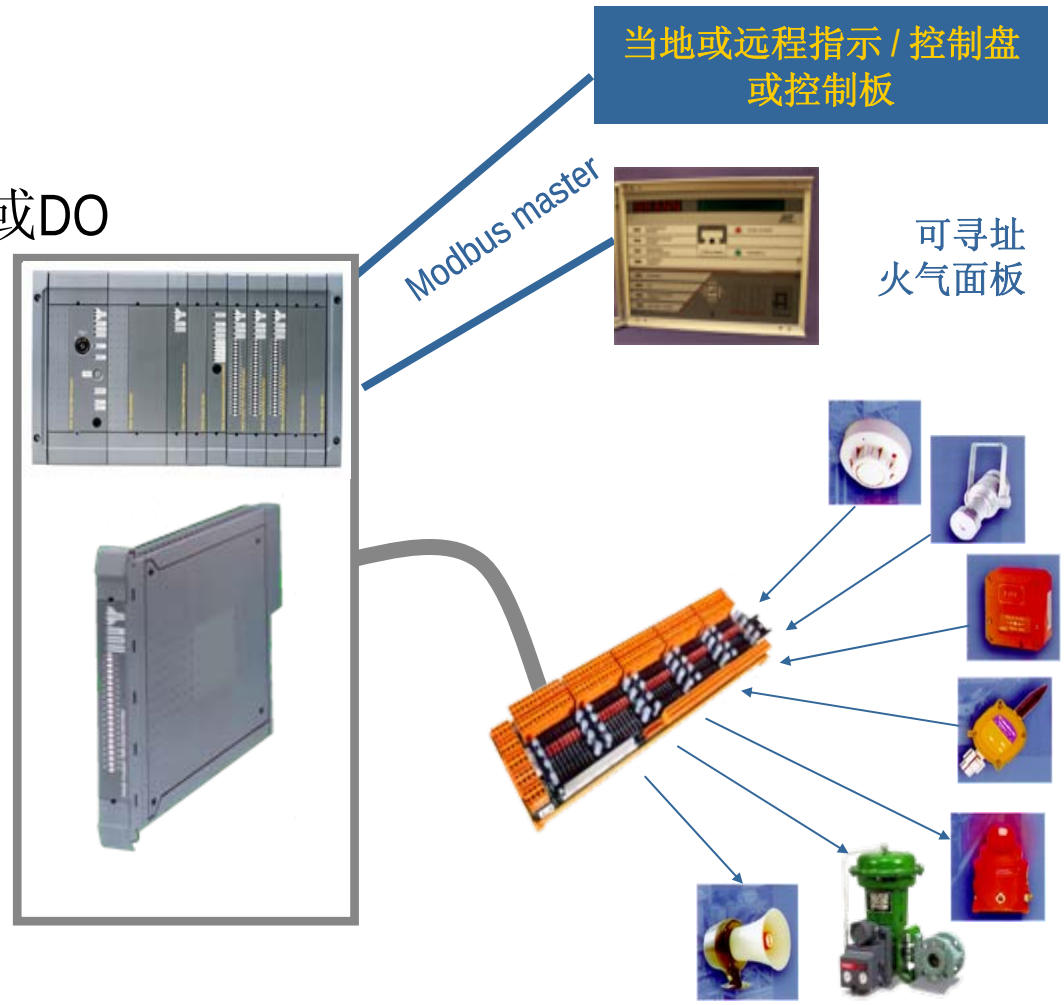
- 三重化(40点)和双重化 (40点) 可选
- 每点三通道，每通道3个A/D转换器
- 门槛值可组态(LL, L, H, HH)并由前面板LED显示
- 每点实现1毫秒SOE分辨率
- 均可热更换
- 环境/现场诊断
- 线监测功能

输出模块

- 每点0.75A或2A输出，模块最大输出30A
- 无需保险丝
- 电压电流值实时显示真正的六元素表决输出
- Stuck on/stuck off测试

Trusted硬件 – 专用I/O模块 （火灾气体F&G）

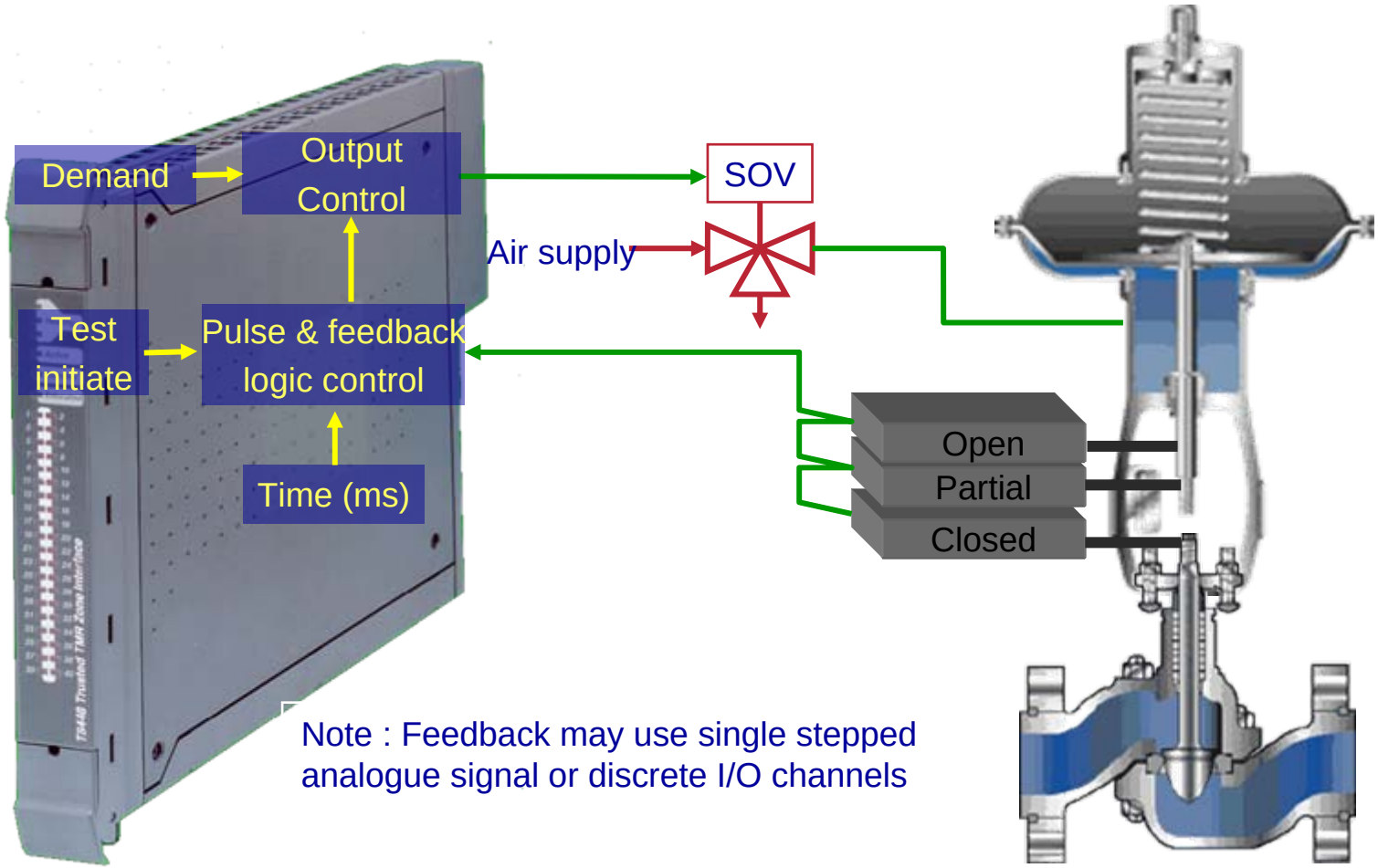
- 独特的通用I/O模块
- 所有I/O均区域隔离
- 40点TMR I/O可为DI、AI、FI或DO
- 在模块上进行火气报警
- 线监测
  - 输入和输出
- 火气回路复位
  - 无需额外硬件
- 在端子板上进行回路选择



Trusted硬件 – 专用I/O模块 （机组控制TMC）

- 9 TMR脉冲输入
- 6 TMR开关量输出
- 高速的超速保护
- 高速的超加速度保护
- 1毫秒SOE – 报警和历史纪录
- <20毫秒响应时间
- OPC和Modbus通讯
- 满足API 670机械保护规范
- 可独立运行

Trusted硬件 – 专用I/O模块 （阀门测试VT）



Trusted软件 – IEC 1131 Toolset（工具箱）

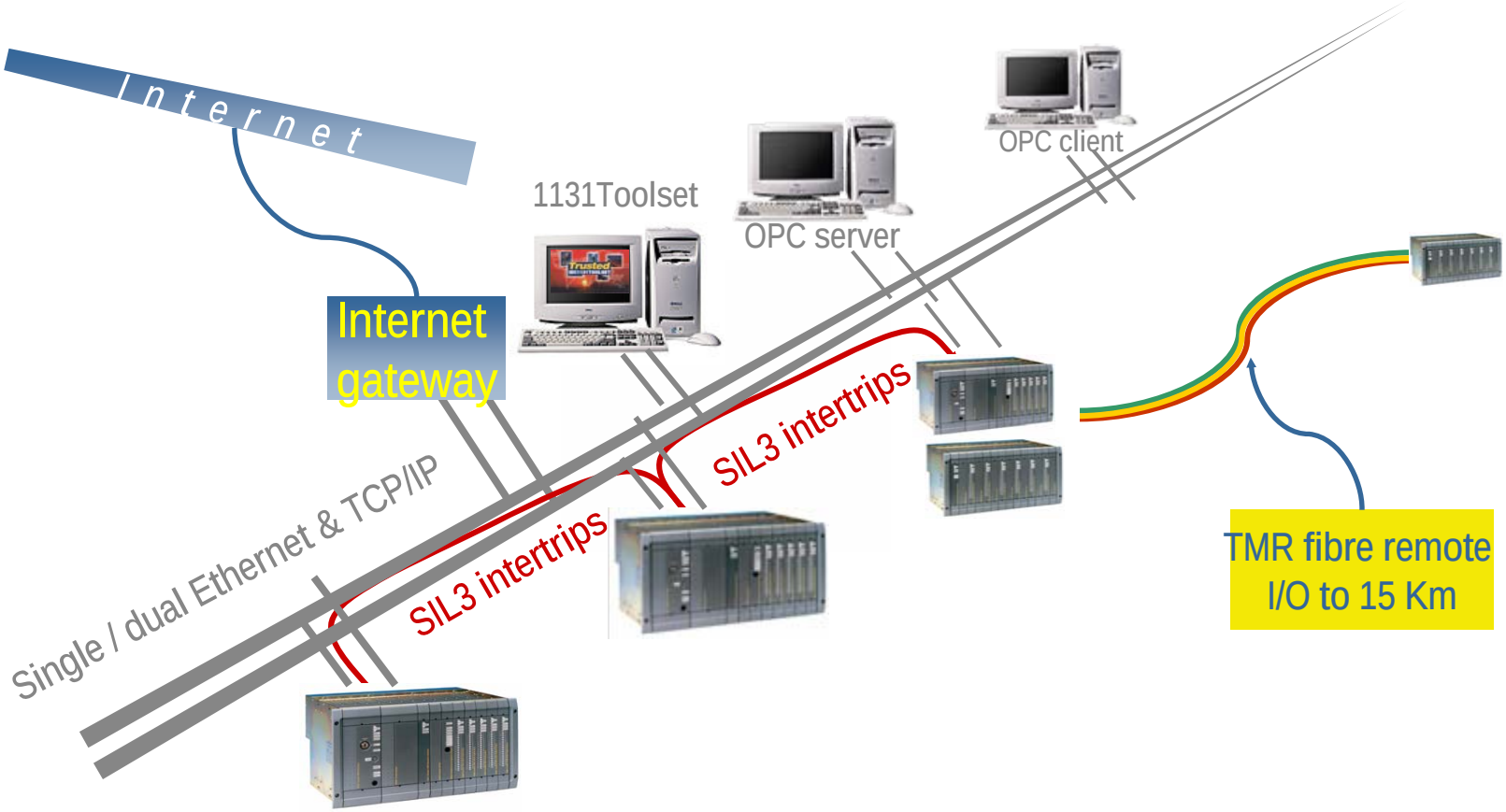
IEC1131 TOOLSET

- Windows NT/XP/2000环境TUV认证
- 也可用于Windows 95/98

用于组态和编程

- 全套5种 IEC1131-3编程语言
- 离线仿真
- 在线监测
- 权限控制
- 版本跟踪
- 数据导入/导出
- 功能库

Trusted 通讯网络



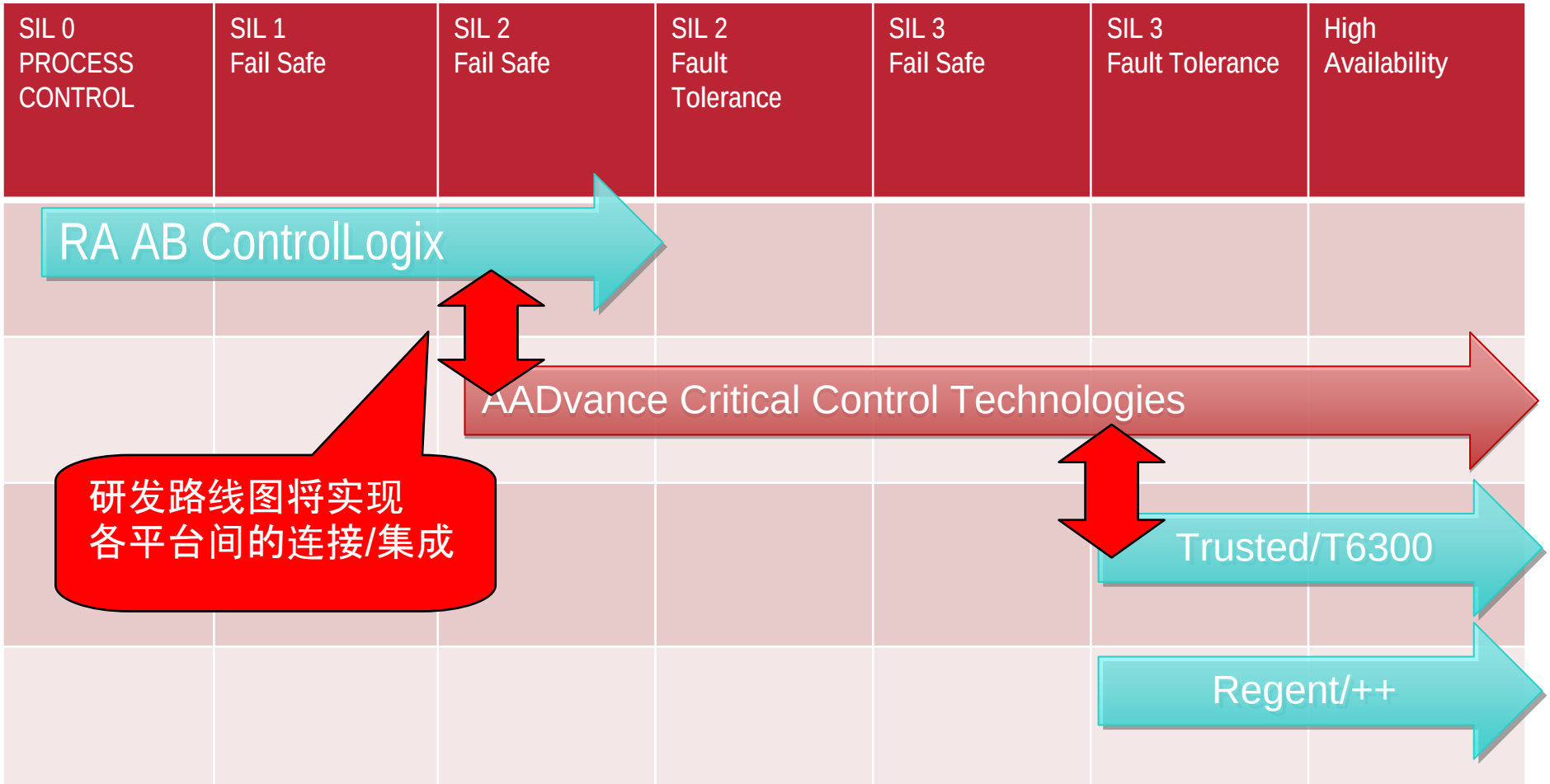
AADvance关键控制系统及环境 - 新生代产品

- 2008年发布
- 用以辅助而非替代Trusted
- 单重化、双重化、三重化
- 可单独成系统或集散式分布
- IEC 61508 认证为SIL 2 (单) 和 SIL 3 (双/三)
- IEC 61131-3 编程环境
- 支持HART、OPC、Modbus等协议

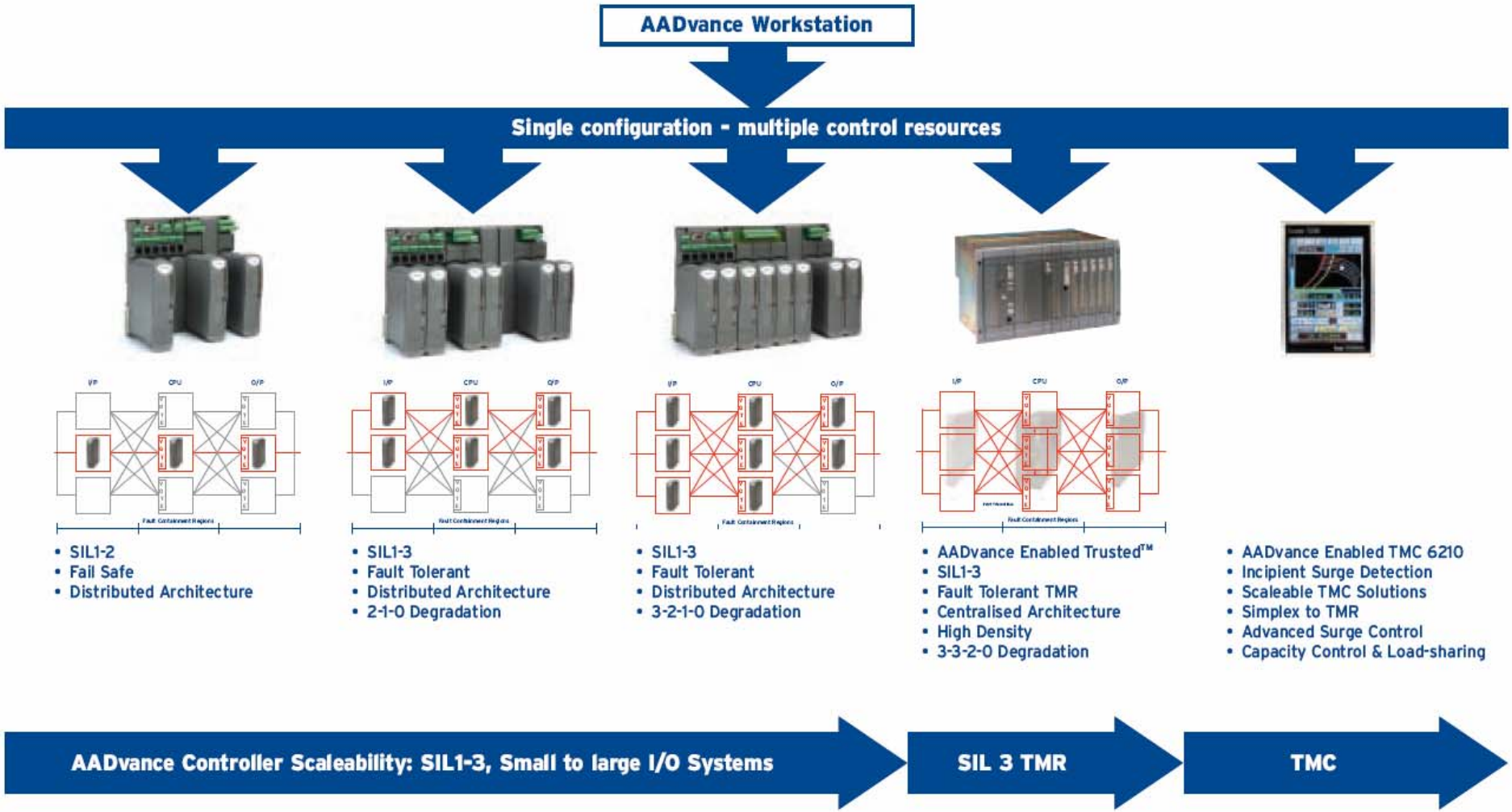
AADvance 并非

- Trusted的替代产品
- 就是 TMR产品
- 仅能 应用于SIL3场合
- 只是 安全系统

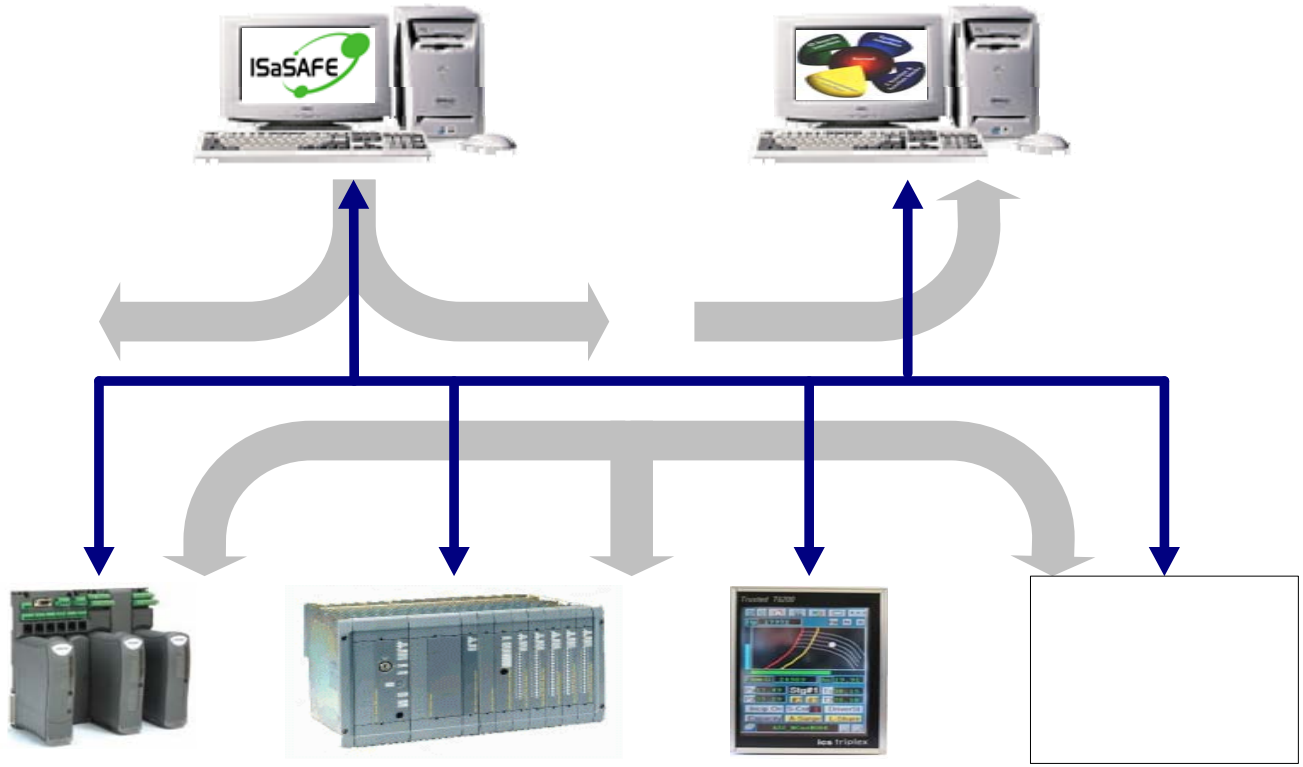
而是...用以填补过程及关键控制方案的空白



AADvance – 硬件配置



AADvance – 软件环境



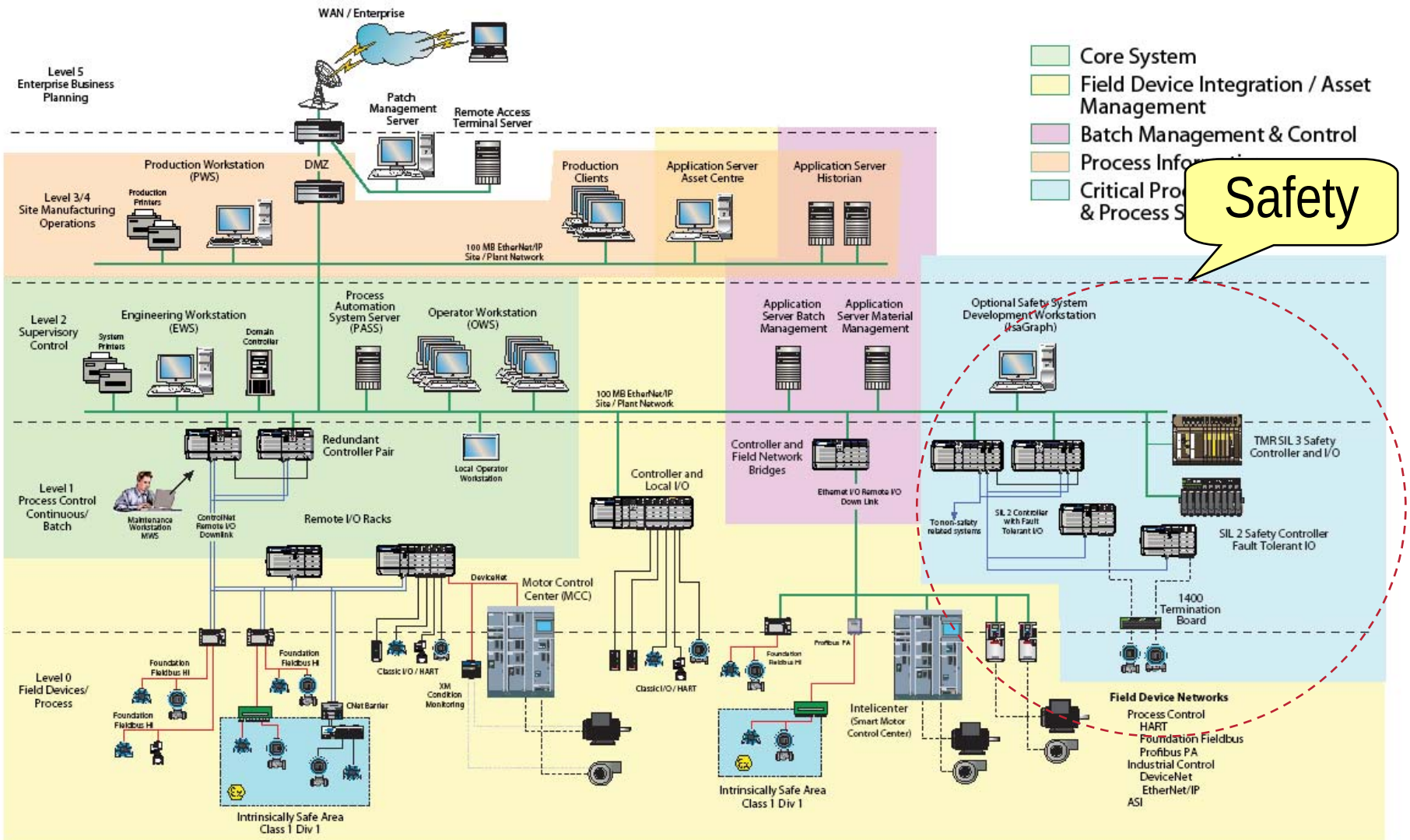
ICS Triplex – 关键控制的梦工厂

RunSafe

Agenda

- 安全定义
- 什么是SIL
- ICS Triplex
- 安全应用

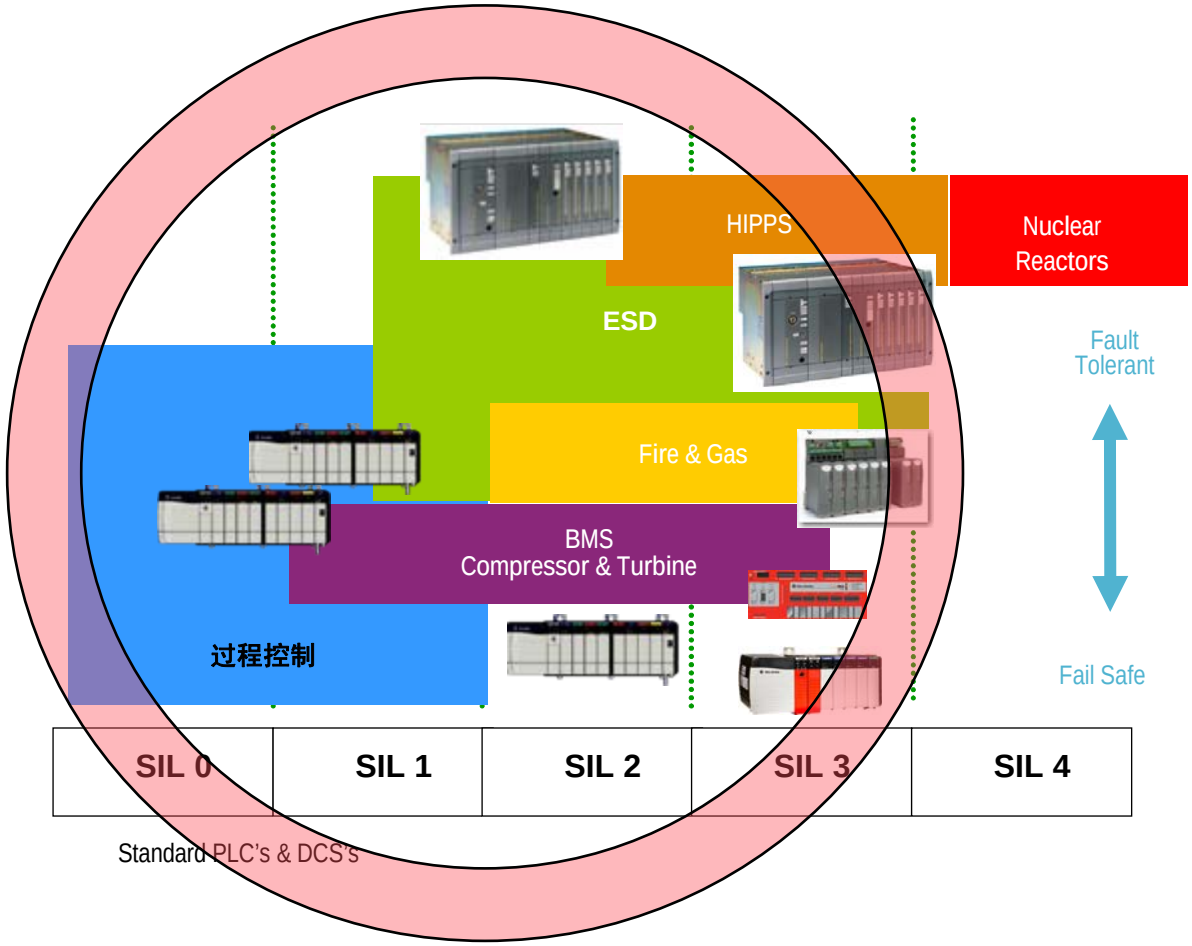
Rockwell Automation PlantPAx Process Automation Functional System Areas



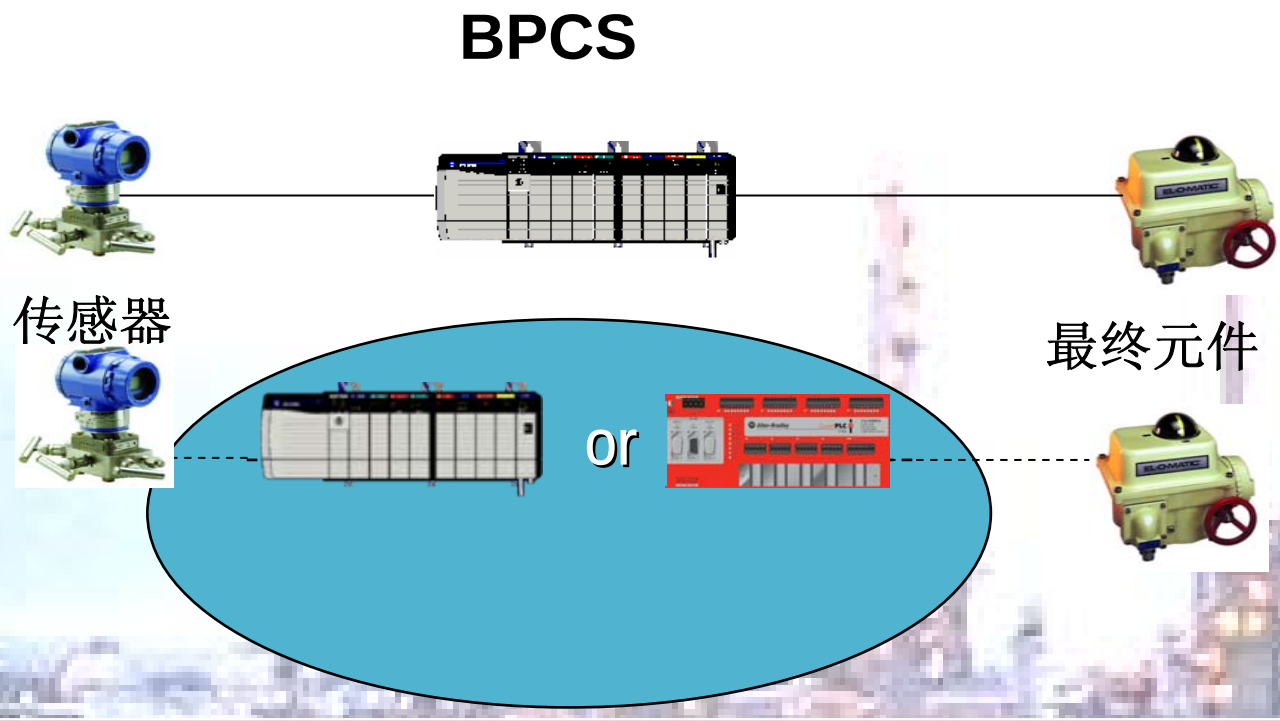
过程控制安全解决方案

- PlantPAx 过程安全解决方案
  - ESD 解决方案
  - 火灾 & 天然气
  - BMS
  - 涡轮透平
  - 其它

PlantPAx: 过程安全能力



ESD(*Emergency Shutdown Device*)
紧急停车系统



ESD紧急停车系统按照安全独立原则要求，独立于集散控制系统，其安全级别高。在正常情况下，ESD系统是处于静态的，不需要人为干预。作为安全保护系统，实时在线监测装置的安全性。只有当生产装置出现紧急情况时，不需要经过集散系统，而直接由ESD发出保护联锁信号，对现场设备进行安全保护，避免危险扩散造成巨大损失

ESD 紧急停车系统

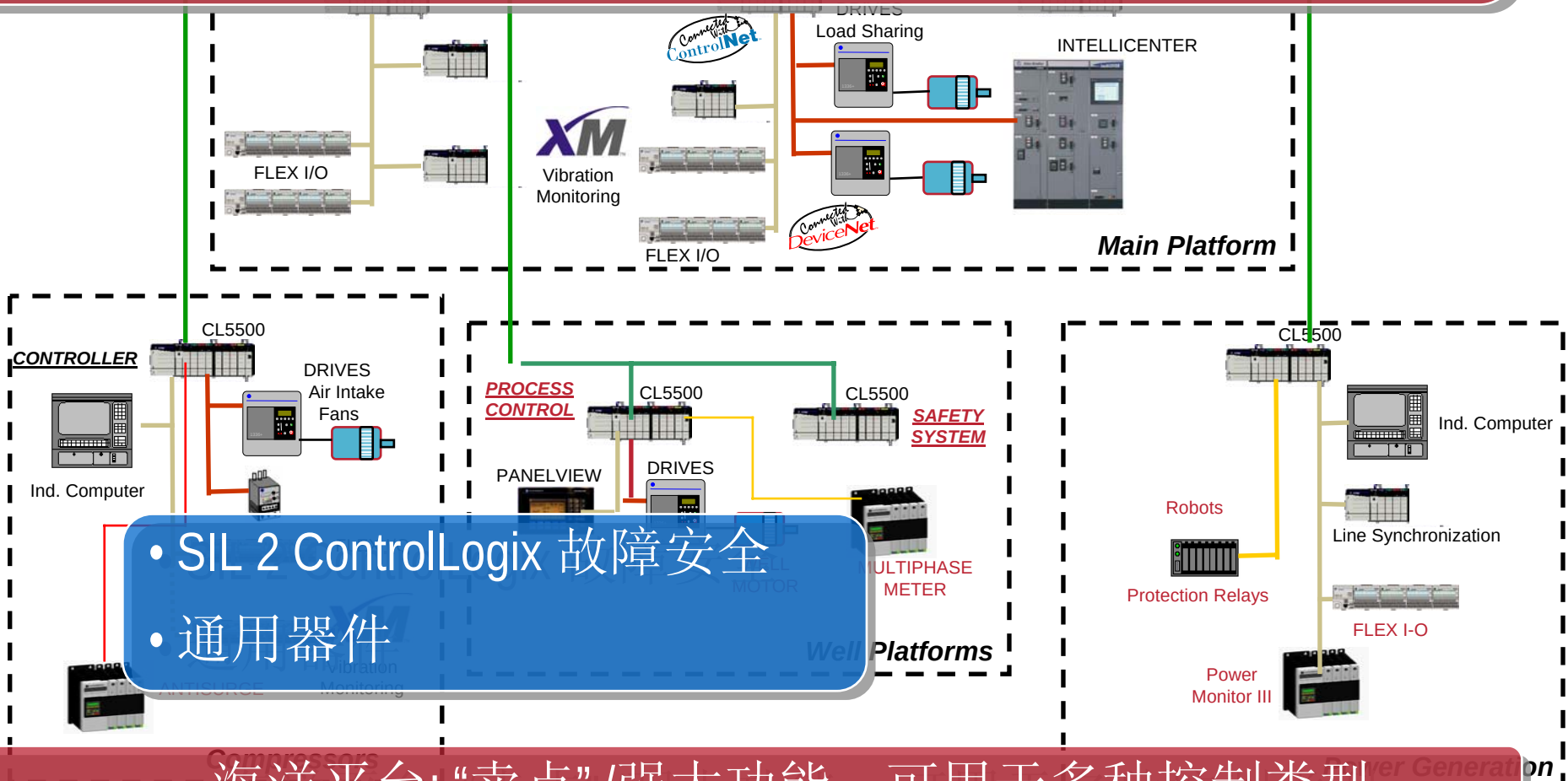
- 安全响应 – 对从故障安全到容错/高可用性
- SIL范围: SIL 1, 2和 3.
- 典型解决方案:
  - 平台
  - 生产工厂
  - 管道、钻井 & 压缩机

- SIL 1或 2 紧急停车,
- SIL 2 SRM用于高可用性/容错
- SIL 3 ICS Triplex

当要求PCS&SIS为通用产品，并更低成本时，可比DCS供应商有优势。

主石油平台控制ESD/PSD

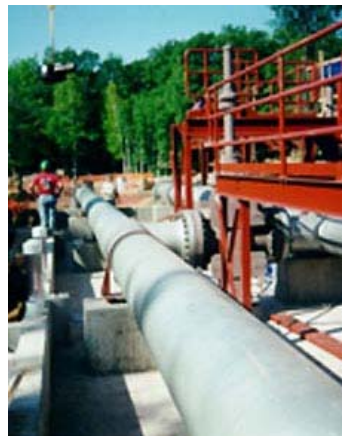
在生产过程中，被处理的介质往往是高温高压、易燃易爆的气体或液体，并且基于海上采油作业的特殊性，一旦发生问题，海上逃生和海上救援难度非常大，人员安全、设备安全和环境安全问题显得更为突出。当系统出现异常的工作状况时，快速可靠的用来实现保护功能的紧急关停装置的作用就更加重要



海洋平台:“卖点”/强大功能，可用于多种控制类型

石油 &天然气管道ESD

- 描述: 管道分布包括:
  - 泵/压缩机站、测量站、关闭阀门、控制系统和SCADA软件。
  - 安全系统通常能够检测压力的高/低
  - ESD将关停泵/压缩机并关闭适当的阀门。
- 通用需求
  - 快速的反应时间。ESD 安装在管道的周围，可能距离较远。
  - 输入通常是模拟量。输出通常是数字量。
- 安全响应: 故障安全
- SIL 服务范围 – SIL 1-2
- 故障停车或者高可用性方案取决于设计规范
-



火灾和气体“系统”

火灾及可燃性气体、有毒气体监控系统（F&Gs）是一种能为火灾探测器供电、接收、显示和传递火灾、气体等报警信号，并能对自动消防等装置发出控制信号的报警装置系统，当火灾、气体探测器探测到火灾后，系统能接受火灾、气体探测器发来的报警信号，迅速、正确地进行转换和处理，并以声光报警形式，指示火灾发生的具体部位，以便及时采取有效的处理措施。

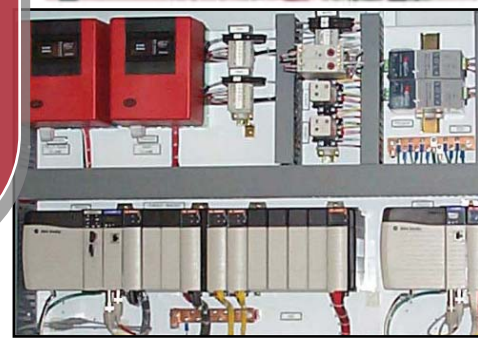
- **特别需求:**
  - FM NFPA 72法规
  - 本质安全安全栅
  - 快速响应
  - 对于许多传感器和检测器的接口,包括火焰、**温度**、二氧化碳、一氧化物、毒气的检测器
  - 排风口、灭火器&其他设备的执行机构
- 安全响应 – 通常情况下高可用性的故障安全，是通过安全设计和多区域、传感器等等来实现的。
- SIL服务范围: SIL 2到 3
- 典型解决方案:
- 机会: 精炼厂，天然气罐/球/容器、管道中的石油或天然气泵站、石油或天然气卡车加油站等等

BMS 燃烧管理系统

- 功能：用于火炉、锅炉和燃烧控制的系统
  - BMS用于火炉和锅炉的安全启动和关闭。
  - 燃烧控制是主系统的一部分。
- SIL服务范围: SIL 1 到3
-

- SIL 2 ControlLogix安全停车
- SIL 3 ICS Triplex

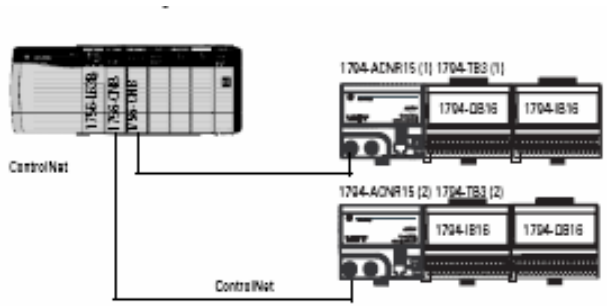
1，点火前炉膛吹扫。
2，油/煤燃烧器控制。
3，风挡板联锁控制。
4，火焰监视。
5，有关辅机的启停和保护
6，主燃料跳闸。
7，减负荷控制。
8，联锁和报警。
9，跳闸原因记录。



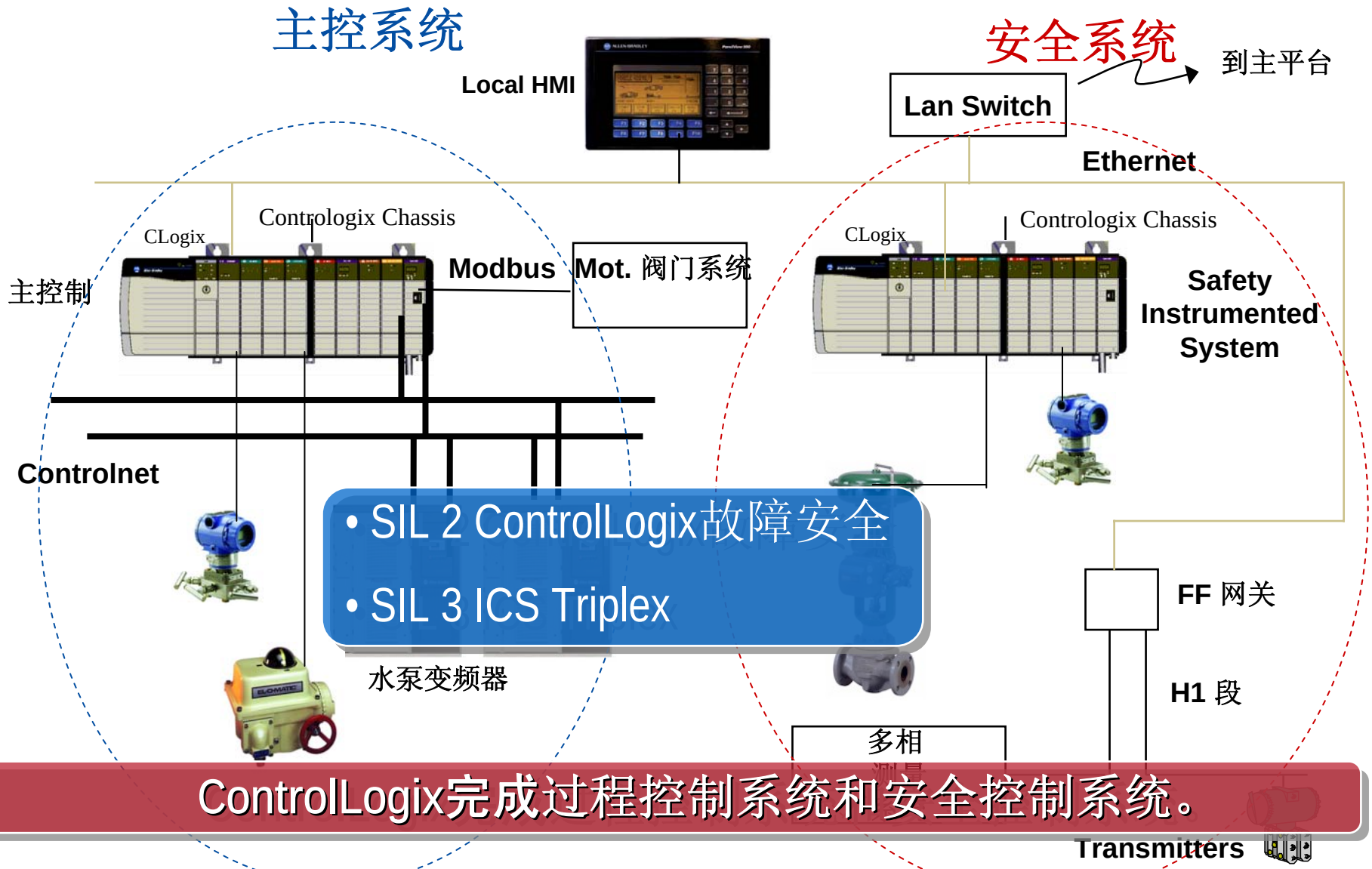
透平控制

- 描述:用于发电和压缩机,水轮机，汽轮机，燃气和燃煤透平
- 需求:
  - 安全响应时间 <10ms
  - 高速模拟信号、热电偶RTD,速度监测
- 安全响应 – 故障安全
- SIL服务范围: SIL 1, 2和 3.
- 典型解决方案:
  - SIL 2 ControlLogix
  - 以及超速监测器。(Entek)

• SIL 2 ControlLogix 故障安全



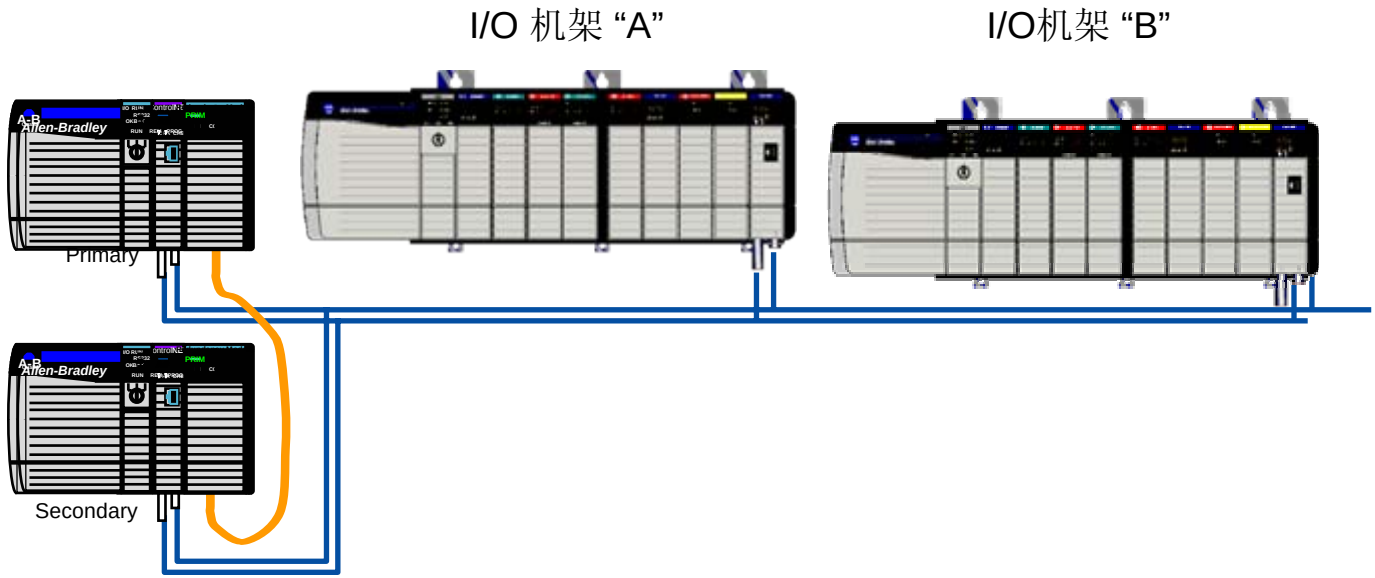
钻井系统



其它安全应用包括:
压缩机、水泵控制

- 描述: 系统用于对于水泵站和压缩机控制提供控制。
  - Shell, Chevron, Compressor Corp
- 特殊需求:
  - 可提供与压力、温度、流量等模拟量信号的接口
  - 可能需要HART或者FieldBus
- 安全响应 – 从故障安全到容错
- SIL等级范围: SIL 1 到 3

经过认证的
冗余产品



- 主、从机架中通过认证的控制器和通讯
- 在各个远程机架（A&B）中相同的 I/O模块布置
- 传感器/执行器都连接到了相同的点/通道，通过接线板连接到每个机架的接口模块
- 周期性脉冲测试是基于预期的系统要求进行的

LISTEN.
THINK.
SOLVE.®

IAU
2009

谢谢！